



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

CH

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,240	06/26/2001	Zheng Qi	BRCMP013A	3459

7590 01/26/2005
CHRISTIE, PARKER & HALE, LLP
P.O. BOX 7068
PASADENA, CA 91109-7068

EXAMINER

PICH, PONNOREAY

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 01/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/892,240

Applicant(s)

QI ET AL. *QI*

Examiner

Ponnoreay Pich

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 6/26/2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-39 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-39 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 June 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>2/14/02, 11/10/03, and 11/8/04</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims 1-39 have been examined and are pending.

Information Disclosure Statement

The examiner has considered the IDS submitted by the applicant.

Specification

The disclosure is objected to because of the following informalities:

1. On page 5, line 14, the applicant discuss Figure 4. Figure 4 does not exist among the drawings submitted by the applicant. Figure 4A and 4B do exist. The applicant may want to consider updating the description in the specification on page 5 to make this clearer.
2. On page 13, the first sentence of the third paragraph states: "As will be appreciated by one of skill the art, various control signals." This sentence appears to be incomplete and the examiner wishes to draw the applicant's attention to it.
3. On page 21, last paragraph, the applicant talks about a "prorogation stage". The examiner is unsure if the applicant meant to say "propagation stage" or really means "prorogation stage". As the claims later refer to a "propagation stage", the examiner will assume the language of the claim is correct during the course of evaluating this application and wish to draw the applicant's attention to this page and paragraph in the specification.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 4, 7, 15, 18, 21, 29, and 33-35 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 1 recites the limitations "the input stage" and "the multiplexer circuitry" in line 5. There are insufficient antecedent basis for these limitations in the claim.
2. Claim 4 recites the limitations "the first level" in line 2 and "the second level" in line 3. There are insufficient antecedent basis for these limitations in the claim.
3. Claim 7 recites the limitation "the output stage" in line 3. There is insufficient antecedent basis for this limitation in the claim.
4. Claim 15 recites the limitations "the input stage" and "the multiplexer circuitry" in line 7. There are insufficient antecedent basis for these limitations in the claim.
5. Claim 18 recites the limitations "the first level" in line 2 and "the second level" in line 3. There are insufficient antecedent basis for these limitations in the claim.
6. Claim 21 recites the limitation "the output stage" in line 3. There is insufficient antecedent basis for this limitation in the claim.

7. Claim 29 recites the limitation "the packets" in line 2. There is insufficient antecedent basis for this limitation in the claim.
8. Claim 33 and 34 recites the limitation "the data path width" in line 2. There is insufficient antecedent basis for this limitation in the claim.
9. Claim 35 recites the limitations "the input buffer size" in line 1 and "the size" in line 2. There are insufficient antecedent basis for these limitations in the claim.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 29 and 38 are rejected under 35 U.S.C. 102(b) as being anticipated by Buer (U.S. 5,697,284).

1. Claim 29: Buer discloses a cryptography engine for performing cryptography operations on a plurality of packets, the plurality of packets having payloads and payload gaps, the cryptography engine comprising:
 - a. A DES engine (col 3, lines 42-55 and col 4, lines 31-65).
 - b. An asynchronous input buffer coupled to the cryptography engine input (col 2, lines 52-67 and col 3, lines 1-8).
 - c. Surrounding logic coupled to the DES engine through the asynchronous input buffer, wherein the DES engine operates at a first clock rate and the

surrounding logic operates at a second clock rate from the first clock rate

(col 2, lines 52-67; col 3, lines 1-8 and lines 42-55; and col 4, lines 31-65).

2. Claim 38: Buer discloses the cryptography engine of claim 29, wherein the DES engine is coupled to surrounding logic, wherein the DES engine runs faster than the surrounding logic (col 5, lines 13-43).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 5-17, and 19-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al (U.S. 6,769,063) in view of Callum (U.S. 6,320,964) and Windirsch (U.S. 6,760,439).

1. Claims 1 and 15: Kanda discloses a cryptographic engine as per claim 1 for performing cryptographic operations on a data block (col 1, lines 8-15).

Kanda also discloses an integrated circuit layout associated with a cryptography engine as per claim 15 for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine (col 1, lines 8-15). Kanda further discloses the cryptographic engine and the integrated circuit layout comprising:

Art Unit: 2135

- a. A key scheduler configured to provide keys for cryptographic operations (col 7, lines 11-25).
- b. Expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block (col 15, lines 8-20 and Figure 8A-8D).
- c. Permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block (col 1, lines 31-46).

Kanda does not explicitly disclose:

- a. A two-level multiplexer.
- b. Expansion logic coupled to an input stage of a multiplexer circuitry.
- c. Permutation logic coupled to the expansion logic.

However, Callum discloses:

- a. A multiplexer circuitry having an input stage and an output stage (Figure 3, items 330, 28, and 64), wherein the keys are provided at the input stage of the multiplexer circuitry (Figure 3, items 330 and KR1-KR4).
- b. Expansion logic coupled to the multiplexer circuitry (Figure 3, items 330 and 319).

- c. Permutation logic coupled to the expansion logic (Figure 3, items 319 and 320).

Further, Windirsch teaches a multiplexer circuitry being a two-level multiplexer (col 1, lines 35-47). One of ordinary skill in the art at the time the applicant's invention was made would have been motivated to employ Callum's teachings with Kanda because as Callum discloses, his teachings would allow a cryptography engine to better handle instruction-intensive bit permutation and thereby achieve greater cryptography speed (Callum's abstract). One of ordinary skill would want to incorporate Windirsch's teachings into the combination system of Kanda and Callum because as Windirsch discloses, it would allow for a single device that can be operated in different ISO-10116 standard modes (col 1, lines 35-67 and col 2, 1st paragraph) and allow for simultaneous processing of a number of data streams (col 2, lines 12-16).

- 2. Claims 2 and 16: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Kanda discloses the cryptographic engine, further comprising an Sbox configuration to alter a third bit sequence corresponding to the portion of the data block by compacting a size of the third bit sequence and altering the third bit sequence using Sbox logic (col 3, lines 31-52; col 10, last paragraph; and col 11, 1st paragraph).
- 3. Claims 3 and 17: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Kanda discloses the

cryptography engine, wherein the cryptography engine is a DES engine (col 14, lines 15-28).

4. Claims 5 and 19: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Kanda discloses the cryptography engine, wherein the first bit sequence is less than 32 bits (col 2, lines 1-21).
5. Claims 6 and 20: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Kanda discloses the cryptography engine, wherein the first bit sequence is four bits (col 17, lines 9-28).
6. Claims 7 and 21: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Callum teaches the cryptography engine, wherein the multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer (col 3, lines 48-61; col 1, lines 39-46; and Fig 3). Windirsch teaches a two-level multiplexer (col 1, lines 35-47). The motivations for combining the teachings of Kanda, Callum, and Windirsch are the same as for claims 1 and 15.
7. Claims 8 and 22: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Callum teaches the cryptography engine, wherein the expansion logic and the permutation logic are associated with DES operations (col 3, lines 32-47 and Fig 3, items 319

and 320). The motivations for combining the teachings of Kanda, Callum, and Windirsch are the same as for claims 1 and 15.

8. Claims 9 and 23: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Further, Windirsch teaches pipelining being used in an encryption/decryption device (col 2, lines 12-35). One of ordinary skill would be motivated to incorporate Windirsch's teachings of pipelining into the combination system of Kanda and Callum for the same reasons as for claims 1 and 15.
9. Claims 10 and 24: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Kanda discloses the cryptography engine, wherein the key scheduler comprises a plurality of stages (col 1, lines 18-67).
10. Claims 11 and 25: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Kanda discloses the cryptography engine, wherein the key scheduler comprises a determination stage (col 15, lines 21-33).
11. Claims 12 and 26: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Callum discloses the cryptography engine, wherein the key scheduler comprises a shift stage (col 4, lines 46-67 and col 5, lines 1-5). Motivations for combining Kanda, Callum, and Windirsch's teachings for claims 12 and 26 are the same as for claims 1 and 15.

12. Claims 13 and 27: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Kanda discloses the cryptography engine, wherein the key scheduler comprises a propagation stage (col 2, lines 1-21).

13. Claims 14 and 28: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. Also, Kanda discloses the cryptography engine, wherein the key scheduler comprises a consumption stage (col 3, lines 30-51).

Claims 4 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al (U.S. 6,769,063) in view of Callum (U.S. 6,320,964), Windirsch (U.S. 6,760,439), and Steinman et al (U.S. 5,91,349).

1. Claims 4 and 18: Kanda, Callum, and Windirsch teach all subject matter as described in claims 1 and 15 respectively. They do not explicitly teach two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on a second level. However, Steinman teaches 2-to-1 multiplexer usage (col 3, last paragraph and col 4, 1st paragraph). It would have been obvious to one of ordinary skill at the time the applicant's invention was made to employ Steinman's teachings within the combination system of Kanda and Callum as it would allow increased performance of a computer memory system by reducing lost clock cycles (Steinman's abstract). It would have been obvious to one of ordinary skill to have two 2-to-1 multiplexers on the first level coupled to two 2-to-1 multiplexers on the second level because it would allow

for increased performance of DES or triple DES engine as the performance of the computer improved in using 2-to-1 multiplexers. The speed up in clock cycle improves the performance of DES.

Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Buer (U.S. 5,671,284) in view of Guski et al (U.S. 5,661,807).

1. Claim 30: Buer teaches all subject matter as described in claim 29. Buer does not teach the cryptography engine coupled to an authentication engine. However, Guski discloses a cryptography engine coupled to an authentication engine (abstract). Guski also teaches that a cryptography engine coupled to an authentication engine was well known at the time the applicant's invention was made (col 1, lines 28-37). One of ordinary skill in the art at the time of the applicant's invention would be motivated to combine Buer and Guski's teachings because as disclosed by Guski, when transmitting passwords between two parties during authentication, the password is vulnerable to being intercepted (col 1, lines 15-27). Encrypting a password or other authentication information before transmission would prevent the authentication information from falling into unauthorized hands (Guski: col 1, lines 15-27).

Claims 31-32 and 35-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buer (U.S. 5,671,284) in view of Windirsch (U.S. 6,760,439).

1. Claim 31: Buer teaches all subject matter as described in claim 29. In addition, Buer teaches the DES engine comprising a multiplexer (col 4, lines

31-65). Buer does not teach a two level multiplexer. However, Windirsch teaches a multiplexer circuitry being a two-level multiplexer (col 1, lines 35-47). One of ordinary skill would want to incorporate Windirsch's teachings with Buer's because as Windirsch discloses, it would allow for a single device that can be operated in different ISO-10116 standard modes (col 1, lines 35-67 and col 2, 1st paragraph) and allow for simultaneous processing of a number of data streams (col 2, lines 12-16).

2. Claim 32: Buer and Windirsch teach all subject matter as described in claim 31. In addition, Buer teaches the cryptography engine further comprising an asynchronous output buffer coupled to the DES engine output (col 5, 2nd paragraph and Fig 4, items 430 and 440).
3. Claim 35: Buer and Windirsch teach all subject matter as described in claim 31. They do not explicitly teach the using the size of the payload gaps and the second clock rate to determine the input buffer size. However, one of ordinary skill at the time the applicant's invention was made would recognize that the rate at which data in the payload portion of the packets can be provided continually to the cryptography engine can be determined using the size of the payload gaps and the second clock rate (the clock rate of the surrounding logic). Knowing this, one of ordinary skill would determine the input buffer size using the payload gap sizes and the rate of the second clock so as to not waste system resources.

4. Claim 36: Buer and Windirsch teach all subject matter as described in claim 31. Buer does not teach the DES engine further comprising a pipelined key scheduler, but Windirsch does (col 2, lines 12-35 and Fig 1, item 5).

Motivation for combining Buer and Windirsch's teachings are the same as for claim 31.

Claims 33 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Buer (U.S. 5,671,284) in view of Windirsch (U.S. 6,760,439) and Pawlowski (U.S. 5,469,547).

1. Claim 33: Buer and Windirsch teach all subject matter as described in claim 31. They do not teach the cryptography engine, wherein the asynchronous input buffer is used to convert a data path width from 32-bits to 64-bits. However, Pawlowski discloses an asynchronous input buffer being used to convert a data path width from 32-bits to 64-bits (col 5, last paragraph and col 6, 1st paragraph). One of ordinary skill at the time the applicant's invention was made would be motivated to incorporate Pawlowski's teachings with Buer and Windirsch because as Pawlowski discloses, doing so would minimize data transfer times within an asynchronous bus transaction (col 1, lines 10-14). The examiner would like to note that the buffer disclosed by Pawlowski is bi-directional, so it can be both an input and output buffer.
2. Claim 34: Buer and Windirsch teach all subject matter as described in claim 31. They do not teach the cryptography engine, wherein the asynchronous output buffer is used to convert a data path width from 64-bits to 32-bits.

However, Pawlowski discloses an asynchronous output buffer being used to convert a data path width from 64-bits to 32-bits (col 5, last paragraph and col 6, 1st paragraph). One of ordinary skill at the time the applicant's invention was made would be motivated to incorporate Pawlowski's teachings with Buer and Windirsch's for the same reason as in claim 33.

Claim 37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Buer (U.S. 5,671,284) in view of Windirsch (U.S. 6,760,439) and Kanda et al (U.S. 6,769,063).

1. Claim 37: Buer and Windirsch teach all subject matter as described in claim 31. They do not teach the DES engine further comprising inverse permutation logic. However, Kanda teaches a DES engine further comprising inverse permutation logic (col 1, lines 30-65). One of ordinary skill in the art at the time the applicant's invention was made would be motivated to incorporate Kanda's teachings into the combination system of Buer and Windirsch as it would increase the cryptography engine's invulnerability against differential cryptanalysis and linear cryptanalysis as disclosed by Kanda (Kanda's abstract).

Claim 39 is rejected under 35 U.S.C. 103(a) as being unpatentable over Buer (U.S. 5,671,284).

1. Claim 39: Buer teaches all subject matter as described in claim 38. Buer does not explicitly teach the DES engine and the surrounding logic running at about 500MHz and about 166MHz, respectively. However, as disclosed in

claim 38, Buer does teach the DES engine running at a higher clock rate than the surrounding logic (col 1, lines 30-65). Further, the applicant has not disclosed that having the DES engine run at about 500MHz and the surrounding logic run at about 166MHz solves any stated problem or is for any particular purpose and the stated clock rates appear to be an arbitrary design consideration which fails to patentably distinguish over Buer.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

1. Luyster (U.S. 6,578,150) discloses encryption using block cipher.
2. Sugahara et al (U.S. 2001/0011251) discloses an authentication engine coupled to a cryptography engine.

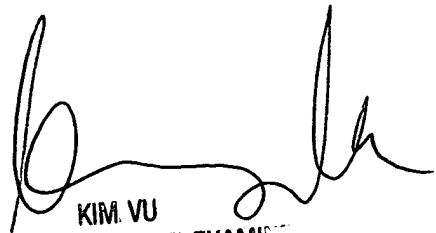
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 21